ABSTRACT OF THE DISCLOSURE

A method for securing a communication between at least one initiator (I) and one responder (R) generates a first key (KEr) within the responder (R), generates a second key (K) within the responder (R), computes an authentication code (C) using the first key (KEr) and the second key within said responder (R), transmits the second key (K) and the authentication code (C) from the responder (R) to the initiator (I) using a first communication channel, transmits the first key (KEr) from the responder (R) to the initiator (I) using a second communication channel, computes a verification code (C') using the first key (KEr) and the second key (K) within the initiator (I), and compares the verification code (C') with the authentication code (C) within the initiator.

Figure 2 for publication